

Autoras:
Carolina Botero Cabrera
Lucía Camacho Gutiérrez

Investigación:
Néstor Espinosa Robledo

Informe

¿DÓNDE ESTÁN MIS DATOS? 2020







Un informe de Fundación Karisma que evalúa el compromiso que los proveedores de internet en Colombia tienen con los derechos a la libertad de expresión, intimidad y seguridad digital de las personas usuarias.



Autoras:
Carolina Botero Cabrera
Lucía Camacho Gutiérrez

Investigación:
Néstor Espinosa Robledo

Un informe de:



Con el apoyo de:



Fundación Karisma hace un reconocimiento especial a otros proyectos similares que han servido como inspiración: **¿Quién defiende tus datos?** de R3D México, **¿Quién defiende tus datos?** de TEDIC Paraguay, **Quem defende seus dados?** de Internet LAB Brasil, **¿Quién defiende tus datos?** de Hiperderecho Perú, **¿Quién defiende tus datos?** de Derechos Digitales Chile, **¿Quién defiende tus datos?** de ADC Digital Argentina. **¿Quién defiende tus datos?** Panamá y, a otros fuera de la región como **¿Quién defiende tus datos?** de Eticas Foundation España, **Who has your back?** de la Electronic Frontier Foundation y **Ranking Digital Rights** del Open Technology Institute.

También agradece a las personas de las empresas evaluadas que se reunieron con el equipo de trabajo de la Fundación y que han estado trabajando en mejorar los resultados de este ejercicio.

Autoras:
Carolina Botero Cabrera
Lucía Camacho Gutiérrez

Investigación:
Néstor Espinosa Robledo

Revisión:
Mariana Lozano
Alejandra Martínez
Juan Diego Castañeda

Coordinación Editorial:
Alejandra Martínez

Diagramación y diseño gráfico:
Hugo Vásquez Echavarría
Daniela Moreno Ramírez

Bogotá, Colombia
Marzo de 2021



CONTENIDO

Informe ¿DÓNDE ESTÁN MIS DATOS

SOBRE EL INFORME

En 2021, después de un año de que comenzara una pandemia en la que la tecnología ha jugado un papel clave, parece más claro que nunca que las discusiones sobre el rol de las empresas intermediarias de internet -especialmente las proveedoras del servicio-, están vigentes. No solo por su papel predominante a la hora de facilitar nuestros derechos humanos en línea que se acentuó por la pandemia, sino porque está claro que hay muchos intereses en regularlas, lo que incluye, por ejemplo, solicitudes indiscriminadas de entidades públicas para acceder a datos de las personas suscriptoras de sus servicios.

Con sus actividades, estas empresas impactan el ejercicio de derechos como el de privacidad y el de libertad de expresión, pues recolectan y custodian una cantidad considerable de datos personales y sensibles de nuestras comunicaciones y además porque pueden incidir sobre lo que consultan y pueden acceder o no las personas cuando navegan por Internet.

Una vez más y desde el año 2016 la Fundación Karisma pública de manera anual su informe "¿Dónde están mis datos?" con el que se propone analizar cómo las principales empresas proveedoras del servicio de internet y telefonía celular en Colombia dicen cumplir sus obligaciones en materia de derechos humanos.

Desde entonces, el objetivo de este informe ha sido el de proveer una herramienta que facilite a las personas usuarias el proceso de toma de decisión cuando contratan dichos servicios y además ofrecer un instrumento que facilite la comprensión sobre aspectos de la tecnología que cada vez más deben ser de interés para las personas.

"¿Dónde están mis datos?" analiza cómo protegen nuestros derechos a la libertad de expresión, intimidad y seguridad digital las siete compañías de internet y telefonía celular más importantes en el país: Claro, Movistar, Tigo, Etb, DirecTv, Emcali y Avantel. El informe evalúa lo que estas compañías dicen hacer a la hora de respetar el ejercicio de los derechos de las personas que usan sus servicios. No se pretende verificar si en efecto cumplen lo que dicen hacer.

El análisis de lo que dicen que hacen esas empresas se lleva a cabo a través de la revisión material de los documentos que son públicos y accesibles en los portales web de cada compañía. Esta revisión comprende dos momentos. El primero, de búsqueda preliminar de la información disponible, que se llevó a cabo en el mes de septiembre del año 2020, seguido por una etapa de análisis de acuerdo con cuatro[1] ejes y catorce[2] criterios que tienen indicadores de

1. Compromisos políticos, intimidad, libertad de expresión y seguridad digital.

2. En compromisos políticos (política de género, política de accesibilidad, informes de transparencia), en intimidad (políticas de protección de datos; informa la obligación legal de retención de datos, informa las razones para responder a solicitudes de información del sector público, procedimiento de entrega de datos al sector público, notificación a las personas sobre la entrega de datos a entidades públicas, y criterios para el tratamiento de datos en relación con aliados comerciales); en libertad de expresión (informa sobre la obligación legal de bloqueo, procedimientos de bloqueo, guía de comportamientos no permitidos); en seguridad digital (informe de fuga de datos personales y acciones de mitigación, uso de protocolo de seguridad https en su sitio web).

que se socializaron con cada empresa evaluada. El segundo momento, comprende la retroalimentación recibida respecto a la calificación preliminar para cada empresa, así como la redacción de nuestro informe final y su publicación en el día internacional del consumidor.

El informe de 2020 realmente se refiere a lo sucedido en 2019 y por tanto, solo en 2021 estaremos abordando un año tan desafiante para las comunicaciones como lo fue el 2020, el de inicio de la pandemia.

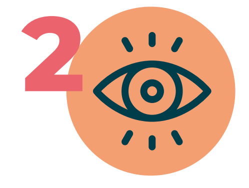
En el informe de 2020 incluimos como nuevo actor a Avantel al darnos cuenta que esa empresa fue incluida por la Comisión de Regulación de las Comunicaciones dentro de las empresas obligadas a informar sobre el tráfico de internet por tener más de 50 mil usuarios en todo el país. Esperamos que este hecho ayude a incentivar una sana competencia por incorporar más y mejores estándares para la protección de los derechos de las personas que usan sus servicios.

Para el informe de este año, nuestra metodología no cambió. Continuamos en esta edición con una evaluación más exigente, pues creemos que luego de cinco años de vigencia de este esfuerzo, hemos generado espacios de conversación e intercambio con las empresas evaluadas que nos permiten pedir un poco más de lo que dice la ley, de cara a la protección de las personas usuarias.

Estos niveles de exigencia que retomamos fueron considerados particularmente en tres de los cuatro ejes que integran nuestra metodología. El de compromisos políticos, el de intimidad y el de libertad de expresión.



En el eje de compromisos políticos. En la revisión del informe de transparencia esperamos nuevamente un mayor nivel de especificidad y desagregación en los datos sobre solicitudes de datos del suscriptor, bloqueos de URL o sitios web, así como interceptaciones de líneas telefónicas con detalle sobre el número de solicitudes elevadas por mes, por año, aquellas que fueron recibidas y atendidas de manera satisfactoria, la temporalidad del bloqueo, la duración de la interceptación, entre otros que detallamos en este eje de nuestra metodología.



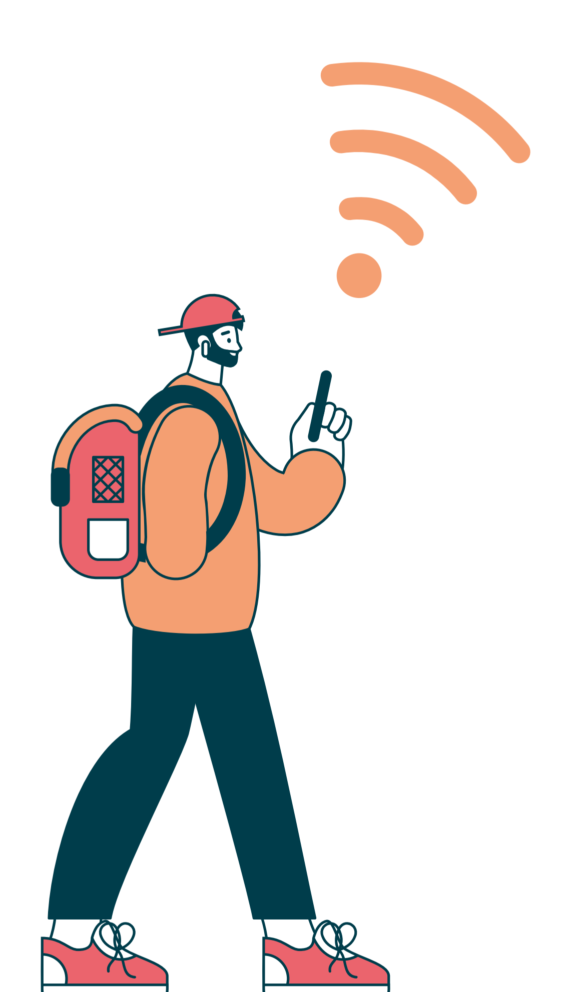
En el eje de intimidad. En la revisión de las políticas de protección de datos esperamos que las empresas proporcionen información más detallada y concreta sobre los datos que recogen de las personas usuarias. Las fórmulas genéricas al estilo “recogemos datos personales” ya no valen. También queremos conocer con precisión los usos que se dan a esos datos personales y el tiempo por el que son retenidos o almacenados.

Esperamos encontrar en las políticas de las empresas criterios para autorizar o denegar las solicitudes de entrega de datos al sector público que especifiquen el proceso desde que se recibe una solicitud de este tipo hasta que se resuelve. Así mismo, esperamos encontrar mecanismos de protección a las personas usuarias que les permita conocer y defenderse de manera temprana sobre las solicitudes de entrega de sus datos personales a terceros, sean éstos autoridades judiciales o aliados comerciales de la empresa proveedora del servicio de internet y telefonía celular.



En el eje de libertad de expresión. En la revisión de las prácticas de bloqueo legal y contractual, evaluamos de manera más detallada los procedimientos con los que se informa a la personas sobre el motivo del bloqueo y si existen mecanismos que les permitan defender sus derechos en caso de tratarse de procedimientos de bloqueo injustos o infundados.

Con la intención de facilitar la lectura de los hallazgos y de hacer comparaciones en el tiempo, la estructura del informe de 2020 se mantiene y gira en torno a las tres preguntas orientadoras que constituyen secciones en nuestro informe: ¿cómo informan las empresas sobre solicitudes de datos personales, interceptación y bloqueos por parte del Estado?, ¿cómo informan las empresas que dan acceso a internet sobre los procesos de entrega de datos al sector público?, y ¿cómo informan sobre sus políticas de protección de datos?



RESUMEN EJECUTIVO DE LOS HALLAZGOS DURANTE 2020

Para resumir los resultados obtenidos en 2020 en comparación con el desempeño que tuvieron las empresas de acuerdo con el informe de 2019, hay que decir que la calificación, en general, no experimentó grandes variaciones. Veamos.

Sobre la pregunta "¿cómo informan las empresas sobre solicitudes de datos personales, interceptación y bloqueos por parte del Estado?", en general, no hubo grandes variaciones con relación a nuestros hallazgos del año anterior. Las empresas todavía no proveen datos comparativos sobre las actividades de entrega de "datos del suscriptor", bloqueos de URL e interceptaciones telefónicas, no hay granularidad en la información sobre cuántas solicitudes de este tipo atienden, cómo las resuelven, y cuál es su duración en el tiempo.

Sobre la pregunta "¿cómo informan las empresas que dan acceso a internet sobre los procesos de entrega de datos al sector público?", en general, encontramos que en la retención de datos, todavía no es una práctica común que se provea información a las personas suscriptoras sobre el marco legal aplicable para tal fin o sobre el tiempo por el que las empresas guardan información sobre las comunicaciones de las personas usuarias; y sobre las solicitudes de datos por el sector público, todavía no es generalizada la entrega de información sobre el procedimiento por el cual se valora la procedencia de estos pedidos, o sobre los mecanismos que tienen las personas para informarse o ser notificadas para poder cuestionarlos y proteger sus derechos.

Sobre la pregunta "¿cómo informan sobre sus políticas de protección de datos?", en general, las políticas de protección de datos todavía pueden mejorar para advertir qué datos concretos recaban las empresas y cuáles son los fines para los que son usados. Las fórmulas genéricas al estilo "recabamos datos sensibles" o "recolectamos datos públicos, semiprivados y privados" no da una idea concreta sobre los datos que se recogen de las personas que suscriben los servicios de estas empresas. Lo mismo aplica con relación a los fines para los que se emplea dicha información.

Y finalmente, en la sección de compromisos políticos, en materia de género y accesibilidad, creemos que es importante seguir avanzando en el diseño y publicación de políticas que favorezcan la diversidad y la inclusión. En seguridad digital, las empresas en general podrían proveer mayor información sobre las estrategias de mitigación ante eventos de fuga de datos, de notificación a las autoridades y a las personas usuarias de sus servicios. Todas sin embargo, han implementado a la fecha el protocolo de seguridad https por lo que no tenemos ninguna variación o desmejora en este criterio.

PRINCIPALES HALLAZGOS

Antes de abordar de lleno las preguntas que orientan la estructura de nuestro informe, queremos dar cuenta del desempeño general de Avantel como nuevo actor que en adelante, será evaluado en "¿Dónde están mis datos?". Esta situación pone de presente que, aun cuando recién ahora entra a ser parte de nuestro informe, lo hace con pie derecho, integrando prácticas e información que le hicieron merecer un buen puntaje en ciertos ejes y criterios.

1 ¿Cómo informan las empresas sobre solicitudes de datos personales, interceptación y bloqueos por parte del Estado?

¿Qué dice la ley?

La ley colombiana no obliga a los operadores a presentar informes de transparencia o informes periódicos sobre los requerimientos que las autoridades hacen de los datos de las personas que usan sus servicios. Sí tienen obligación de entregar información pero sobre los planes de internet y telefonía celular o las prácticas de gestión de tráfico. Sin embargo, dar información sobre lo que sucede con los datos que recolectan se ha convertido en una buena práctica internacional especialmente entre las empresas del sector de las Tecnologías de la Información y las Comunicaciones -TIC-.

Ahora bien, como responsables del tratamiento de datos personales, los operadores sí tienen obligaciones de informar con claridad qué datos recogen y cómo los usan, así como de tener una política de tratamiento de datos. En esta parte de la evaluación sólo analizamos qué datos presenta la empresa respecto a las solicitudes que recibe de parte del Estado en relación con el acceso a datos de las personas usuarias, interceptación de comunicaciones y el bloqueo de URL.

¿Cómo informan los operadores?

En esta evaluación nos interesan tres tipos de peticiones o solicitudes que pueden elevar las entidades del Estado a los proveedores de internet y telefonía celular que son (i) la entrega de datos de las personas suscriptoras, (ii) las solicitudes de interceptaciones a líneas telefónicas y (iii) los bloqueos de URL o sitios web.

Ante estos tres tipos de solicitudes que impactan en la privacidad y libertad de expresión de las personas usuarias de las empresas, esperamos que éstas de manera pública y accesible relacionen el número de solicitudes recibidas por mes o año, las autoridades que efectúan estos pedidos, así como la relación de cuáles y cuántas solicitudes fueron atendidas de manera favorable y cuál terminó siendo su extensión en el tiempo.

Esta información la consultamos directamente en los informes de transparencia o informes anuales de cada empresa, incluso en informes que han recibido el nombre de transparencia sobre el tratamiento de datos. Sin lugar a duda, que cada proveedor de internet y telefonía celular presente un balance sobre este tipo de solicitudes constituye una buena práctica de cara a las personas que usan sus servicios, aun cuando la ley colombiana no obliga a ello.

En línea con nuestro informe del año anterior, vemos que las empresas han incorporado este ejercicio de transparencia al de los informes anuales donde se hacen los balances de tipo financiero. Valdría la pena pensar en mecanismos para que sus informes resalten o separen en forma más evidente esa transparencia económica de la información sobre cómo protegen los derechos de las personas usuarias.

En general, las empresas han adoptado estos informes de transparencia en materia de protección de derechos humanos pero aún no lo hacen entregando datos comparables que permitan tener una mayor idea sobre este tipo de solicitudes.

En 2019, **Movistar** fue la única que cumplió con informar de manera plena y desagregada sobre las solicitudes de datos de las personas que se suscriben a sus servicios, los bloqueos de URL o sitios web, y de interceptaciones de líneas telefónicas fijas.

Claro informa que entrega sus datos por motivos de interceptaciones telefónicas, o con expresiones más generalizadas al indicar que entrega los datos de las personas que se suscriben a sus servicios, pero solo desagrega la información que se relaciona con las solicitudes de bloqueos de URL o sitios web.

Tigo desagregaba información sobre las solicitudes de datos por entidades públicas y solicitudes anuales de interceptaciones concedidas a líneas fijas en el informe anterior (2019) pero no lo hizo este año. Por tanto, su puntaje disminuyó. Este año no encontramos la relación de información sobre bloqueos a sitios web o URL, datos que tampoco identificamos para el informe de 2019.

Por su parte **ETB**, en 2019 no publicó su tradicional informe de transparencia de datos -de hecho era la única empresa que ofrecía este informe con corte semestral-, lo que sin duda impactó negativamente en el análisis de este eje en el que en años anteriores se destacaba al proveer información sobre solicitudes de datos por entidad pública, de bloqueos de sitios web o URL, así como el balance de solicitudes que procedieron y las que fueron negadas en cada evento.

Una vez más, ni **DirecTV** ni **EmCali** publicaron un informe de transparencia o informes relacionados que provean información sobre (i) la entrega de datos de las personas suscriptoras, (ii) las solicitudes de interceptaciones a líneas telefónicas y (iii) los bloqueos de URL o sitios web; por lo que su puntaje no presenta ninguna mejora con relación a los años anteriores.

DirecTV tiene, sin embargo, publicado un procedimiento de bloqueo que se refiere en exclusivo a contenido asociado al abuso y la pornografía infantil. No relaciona cómo opera el procedimiento con relación a otro tipo de bloqueos, ni la dependencia interna que tramita estas peticiones o el número de solicitudes recibidas y el sentido de la respuesta que provee la compañía.

Avantel no cuenta con informes de transparencia en este sentido por lo que esperamos pueda integrarlo para el próximo ciclo de evaluación.

RECOMENDACIONES

1 Reiteramos la sugerencia del año pasado invitando a las empresas a proveer mayores detalles sobre qué entienden por "datos del suscriptor", las entidades que hacen las solicitudes, la indicación de los motivos de solicitud de datos por parte de esas entidades públicas y cuál fue la decisión del operador. También en el caso de bloqueos de sitios y URL recomendamos informar sobre quiénes presentan las solicitudes y sus motivos, discriminando entre bloqueos temporales y permanentes de URL y si se presentaron bloqueos equivocados y las razones.

2 Con la certeza de que este ejercicio desarrolla buenas prácticas internacionales, es importante no retroceder en el terreno ganado. Al respecto, esperamos que ETB retome su informe sobre transparencia de datos con la que lideró por varios años este eje de evaluación. Lo mismo deseamos que suceda con Tigo.

3 Invitamos a DirecTV a hacer un informe específico para Colombia en donde recoja como mínimo la información que otros operadores publican en sus distintos informes.

4 Desearíamos que EmCali elaborara un informe en el que detalle información sobre su compromiso en la protección del derecho a la privacidad y libertad de expresión de las personas usuarias ya que a la fecha en dicho reporte relaciona balances financieros de la compañía.

5 Avantel podría igualmente implementar un informe de transparencia con la información que creemos es de interés de las personas usuarias y esperamos progresivamente ver mejoras en este eje de evaluación.

2 ¿Cómo informan las empresas que dan acceso a internet sobre los procesos de entrega de datos al sector público?

RETENCIÓN DE DATOS

¿Qué dice la ley?

Cuando hablamos de retención de datos nos referimos específicamente a la obligación que tienen los operadores de conservar y entregar a las autoridades de inteligencia y a la Fiscalía General, la información que producen los celulares en relación con el servicio de telecomunicaciones.

Los operadores deben colaborar con la Fiscalía General de la Nación para entregar, en el marco de una investigación penal, los siguientes datos[3]:

1. Los datos de la persona suscriptora, tales como identidad, dirección de facturación y tipo de conexión. Además deben conservarla por cinco años.

2. Información específica contenida en sus bases de datos, tal como sectores, coordenadas geográficas y potencia, entre otras, que contribuya a determinar la ubicación geográfica de los equipos terminales o dispositivos que intervienen en la comunicación. Deben suministrarla en tiempo real en caso de que se requiera.

La ley de Inteligencia y contrainteligencia obliga a los operadores a entregar a agencias de inteligencia[4];

1. El historial de comunicaciones de los abonados telefónicos vinculados, es decir, de las personas que contratan sus servicios.

2. Los datos técnicos de identificación de los suscriptores sobre los que recae la operación.

3. La localización de las celdas en que se encuentran las terminales y cualquier otra información que contribuya a su localización.

3. Decreto 1704 de 2012, artículo 4.

4. Ley 1621 de 2013, artículo 44.

Sin embargo, de toda la información que pueden producir los operadores sobre la actividad de los celulares, no está claro exactamente qué entregan a las autoridades de investigación penal e inteligencia cuando deben cumplir con estas normas. Por eso, en esta pregunta nos preocupamos por cómo informan:

1. A las personas usuarias sobre la existencia de esta obligación.
2. Sobre qué datos retienen en concreto.
3. Sobre el tiempo por el cual los retienen.

Además de las normas de retención de datos que acabamos de exponer, la Fiscalía puede realizar la "búsqueda selectiva en bases de datos"[5] y las autoridades, en general, pueden solicitar datos personales sin autorización del titular, siempre que sea en ejercicio de sus funciones[6]. No está claro cómo funcionan en la práctica cada una de estas facultades ni cómo se relacionan entre ellas.

¿Cómo informan los operadores?

En esta sección revisamos la forma como los operadores informan que desarrollan su obligación de retención de datos, cuáles son los que retienen y por cuánto tiempo. No revisamos el resultado de la actividad de retención de datos. Por ejemplo, el tipo de datos de las personas usuarias que fueron entregados en efecto a la Fiscalía.

Esperamos encontrar esta información en las políticas de protección de datos de las empresas o en los informes de transparencia. La publicación de esta información de manera desagregada para informar debidamente a las personas suscriptoras constituye sin duda una buena práctica

En términos generales, en materia de retención de datos esperamos que los proveedores del servicio de internet y telefonía celular nos cuenten en detalle cuál es el marco legal que aplican en el cumplimiento del deber de retención de datos, qué datos en concreto retienen y por cuánto tiempo.

5. Ley 906 de 2004. Código de Procedimiento Penal. Artículo 244.

6. Ley 1581 de 2012. Artículos 10 y 13.

Luego de revisar las prácticas de las empresas, la mayoría de los operadores informan sobre el cumplimiento de la ley -con o sin la indicación del marco legal al que hacen referencia-, o publican que deben retener los datos de las personas usuarias. Sobre los datos que conservan para entregar a las autoridades en investigaciones penales o de inteligencia o el tiempo que dura la retención, los operadores para 2019 no ampliaron la información, por tanto el informe de 2020 no tiene mayores cambios, en general las empresas en Colombia no son claras en los detalles de esta obligación legal. Veamos.

Claro, **Movistar** y **Tigo** informan que están obligadas por ley a retener datos en indicación del marco legal. **ETB** menciona en su política de tratamiento de datos que retiene datos sin indicación del marco legal.

Claro vuelve a ser la única que advierte el tiempo por el que retiene datos, el cual se extiende hasta por 10 años, al parecer tomando el plazo de retención de los archivos de tipo contable sin que se explique muy la razón para ello.

Movistar cita a plenitud el marco legal que justifica la retención de datos. Incluyen la Ley 906 de 2004 (art. 235), Ley 1621 de 2013 (art. 44), y el Decreto 1704 de 2012 (art. 18). Ese marco legal describe el tiempo de retención que se extiende hasta por cinco años, el tipo de datos que son retenidos (metadatos como el historial de comunicaciones de los suscriptores, su identificación, datos que faciliten su localización, entre otros).

Tigo por su parte informa que tiene un deber legal de retención de datos sin especificar el marco legal en que se funda ese deber. Cuando se trata de detallar el tiempo por el que hace la retención de dichos datos, señala que lo hará por un periodo superior al autorizado por la persona titular de los datos sin la advertencia de un plazo determinado en el tiempo.

ETB emplea una fórmula más bien genérica para señalar, por ejemplo, que retendrá los datos por el tiempo que sea necesario hacerlo.

Por último, **DirecTV**, **EmCali** ni **Avantel** relacionan información sobre el deber legal de retención de datos, sobre el tipo de datos que retienen, ni el tiempo por el que lo hacen.

RECOMENDACIONES

1. Reiteramos las recomendaciones que efectuamos en este sentido en nuestro informe de 2019 al decir que la transparencia en la información en estas actividades de retención de datos es vital para facilitar el derecho de las personas usuarias a mantener un mejor control de su información y el tratamiento que se da a sus datos por terceros en tanto que son actividades que impactan en la protección de su privacidad. Recomendamos que las empresas indiquen con claridad el marco legal que les aplica y los tiempos de retención de datos que se derivan de estas obligaciones legales.

SOLICITUDES POR PARTE DE ENTIDADES PÚBLICAS

¿Qué dice la ley?

La Ley de Protección de Datos[7] permite la entrega de datos personales a entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial sin autorización de la persona titular de los datos. Las autoridades que reciben la información deben guardarla en reserva, usarla sólo para los fines para los cuales la recibieron, deben informar a los titulares del dato sobre el uso que le dan y tomar medidas de seguridad para protegerla[8].

¿Qué informan los operadores?

En este eje de evaluación esperamos que las empresas provean información sobre los procedimientos que han diseñado y que siguen internamente a la hora de entregar datos de las personas que se suscriben a sus servicios a las entidades públicas que los solicitan. Por procedimiento interno nos referimos al proceso de consideración sobre la legalidad y procedencia del pedido antes que al procedimiento desde un punto de vista técnico. Es decir, se trata de establecer si la empresa tiene procedimientos alineados con los derechos humanos.

En términos generales, creemos que todavía falta avanzar tanto en la relación de mayor información sobre las prácticas que emplean a nivel interno los proveedores del servicio de internet y telefonía celular, como en la información sobre la existencia o no de mecanismos que permitan a las personas usuarias de sus servicios enterarse de la entrega de sus datos a entidades públicas. Puede que los haya, tanto procedimientos como mecanismos de este tipo, pero los operadores no informan sus prácticas públicamente.

Valoramos como una buena práctica, que las empresas tengan mecanismos de notificación a las personas usuarias de sus servicios cuando estos procesos de entrega de sus datos se han dado, así como la existencia de mecanismos internos a cargo de funcionarios de la empresa -como por ejemplo, los oficiales de protección de datos- que tienen como propósito proteger los derechos de las personas que suscriben sus servicios ante solicitudes que se consideren injustificadas o excesivas. Veamos.

Solo cuatro de las siete empresas evaluadas cuentan con un protocolo o criterios más o menos definidos para atender estas solicitudes y su procedencia: **Claro**, **Movistar**, **Tigo**, **DirecTV** y **ETB**. Por su cuenta, **Avantel** dice tener procedimientos de este tipo pero no los desarrolla ni explica. EmCali no provee ninguna información al respecto.

7. Ley 1581 de 2012 art. 10 y 13

8. Corte Constitucional. Sentencia C-748 de 2011. M.P. Jorge Ignacio Pretelt Chaljub.

Claro señala en su informe de sostenibilidad que es su deber legal atender las solicitudes de este tipo. En 2019 como en los dos años anteriores esta empresa publicó información sobre los eventos en que puede operar la entrega de datos personales de sus clientes a las autoridades y el marco legal en el que dicha entrega puede sustentarse.

Sin embargo, **Claro** no provee información sobre su procedimiento de entrega de datos que permita entender las fases por las que transcurre un pedido de esta naturaleza, ni el tiempo que una petición de este tipo dura en ser resuelta o la dependencia interna encargada de decidir.

Movistar informa del proceso de gestión de la solicitud de entrega de datos que se radica en la ventanilla "Morato" -que no sabemos si es de radicación en físico o vía web-, en donde se efectúa una validación y en caso de que se determine su procedencia, se clasifica, gestiona y envía. La compañía relaciona además las razones por las que entrega los datos de las personas que usan sus servicios cuando se presentan solicitudes de entes públicos con facultad para ello.

En un documento sobre la gestión de requerimientos de datos personales, **Tigo** prevé un proceso mediante el cual la solicitud ingresa por distintas vías como la inspección judicial, vía web o email -entre otros-; se verifica y valida el contenido de la solicitud, seguido de una búsqueda en bases de datos. Se genera una respuesta para su radicación y posterior envío. No se menciona si hay instancias al interior de la empresa que velen por los derechos de las personas que usan sus servicios.

ETB señala en su política de tratamiento de datos que los requerimientos de datos por autoridades judiciales, administrativas o vigilantes del sector de las telecomunicaciones procederán si se han efectuado en ejercicio de sus funciones legales. Así mismo, que el área encargada de tramitar y verificar la solicitud es la Dirección de Experiencia Back Office que debe dejar registro de las solicitudes así como de las respuestas.

DirecTV es la única empresa que de manera expresa dice que notifica a las personas suscritas en sus servicios ante la gestión de solicitudes de entrega de datos de sus datos así: "nosotros le proveeremos notificación previa de dicho requerimiento y orden de modo que usted pueda impugnarla en un procedimiento antes (sic) los entes", tal y como lo señala en su política de protección de datos. En nuestros informes anteriores, habíamos dado cuenta de esta actividad que era en todo caso facultativa y que ahora, con esta previsión, sin duda constituirá en adelante un compromiso de la compañía.

Este sin duda es el reflejo de lo que consideramos una buena práctica que abre la posibilidad a que las personas que usan sus servicios cuenten con mecanismos de impugnación que les permita en forma más oportuna controvertir órdenes que impactan en su privacidad.

Tratándose de los mecanismos de protección de la privacidad de la persona usuaria ante solicitudes de sus datos efectuadas de manera general, sin duda **Avantel** merece ser vista de cerca. Al respecto queremos resaltar el mecanismo ideado por esta compañía y que denomina como "análisis de impacto en privacidad frente a la autoridad".

El "análisis de impacto en privacidad frente a la autoridad" es un proceso que analiza la manera en que se cumple la ley de cara al tratamiento de datos de las personas suscriptoras de **Avantel**, para prevenir posibles sanciones por la autoridad de protección de datos. Creemos que valdría la pena que estos análisis de impacto en la privacidad tengan lugar especialmente de cara a las solicitudes de datos efectuadas por entidades públicas, y que los criterios que orientan dichos análisis sean en consecuencia de conocimiento para el público.

RECOMENDACIONES

1. Creemos que las empresas deben indicar que cuentan no solo con procedimientos internos para atender las solicitudes de datos personales por parte de las entidades públicas, sino que además pueden incluir detalles sobre la forma como se valora la legalidad, necesidad y proporcionalidad de esas solicitudes.

2. Reiteramos que para dar mejores garantías el procedimiento de entrega de datos, se debe incluir mecanismos de protección de los derechos de las personas usuarias de los servicios de las empresas. Por ejemplo, la afirmación y compromiso de que hay una persona al interior de la empresa que está encargada de revisar las solicitudes para garantizar que se respeten los derechos de las personas suscriptoras de los servicios de las empresas.

3. Pero, hay otros mecanismos, reconocidos a nivel internacional, que pueden servir para mejorar las garantías de respeto a los derechos de quienes suscriben sus servicios, la notificación a las personas usuarias de que sus datos fueron solicitados por entidades públicas permiten a esas personas entender y actuar frente a estas solicitudes, por tanto es una buena práctica que debería no solo ser un compromiso de las empresas, también debería ser implementada en consecuencia.

3 ¿Cómo informan sobre sus políticas de protección de datos?

¿Qué dice la ley?

Los datos personales sólo se pueden usar cuando la persona titular de los mismos ha sido informada sobre el empleo que le darán y ha dado su consentimiento[9]. La ley de protección de datos obliga a quien haga su tratamiento a tener una política de protección de los mismos, además debe solicitar autorización para ese tratamiento[10].

¿Cómo informan los operadores?

En este eje de evaluación analizamos las políticas de protección de datos que los operadores incluyen en sus sitios web. En nuestro informe del año pasado dimos cuenta de cómo desde el año 2015 la confección de estas políticas se refinó. Para entonces, muchas empresas copiaban y pegaban extensos apartados de la Ley 1581 de 2012 de protección de datos.

Hoy en día, nuestro balance nos permite apuntar que el panorama ha cambiado, las políticas de privacidad y protección de datos de las empresas son documentos que explican sus compromisos, se pueden encontrar y navegar más fácilmente, además están escritos en un lenguaje más o menos comprensible para las personas.

Sin embargo, todavía hay espacio de mejora, se necesitan ajustes para acatar los estándares de la autoridad de protección de datos en la materia, por ejemplo, en torno a la necesidad de que se advierta a la persona titular del dato qué datos personales y datos sensibles se están recolectando, cuáles son sus usos, qué terceros podrán acceder a esos datos, adicionalmente -y aun cuando la ley no lo exige- creemos también que sería muy positivo que se advirtiera cuáles son los criterios que orientan o condicionan el acceso de aliados comerciales a esa información que se encuentra en poder de los operadores.

Claro tiene una política de protección de datos que advierte las finalidades del tratamiento pero no desagrega puntualmente los tipos de datos que recoge, aun cuando señala que recoge datos de tipo público, semiprivado y privado. Sobre la manera en que comparte datos con aliados comerciales no tiene ninguna previsión concreta.

9. Ley 1581 de 2012. Ley de protección de datos, artículos 4 y 8 sobre consentimiento y el derecho a ser informado sobre qué uso dan los responsables del tratamiento a los datos personales que capturan y administran.

10. Ley 1581 de 2012. Ley de protección de datos. Artículos 12 y 17 sobre el deber de informar a las personas qué tratamiento dan a sus datos, para qué se recogen sus datos y qué derechos tiene en relación con este tratamiento de datos.

Movistar tiene una política de protección de datos que cuenta con una "sección de interés" que desagrega en detalle los datos que recogen como "datos demográficos, económicos, biométricos, de servicios, comerciales y de localización". Advierten el uso que dan a los datos al señalar que se encuentran "el cálculo de riesgo económico o crediticio, la publicación de directorios, la prevención y control de fraudes" aunque entendemos que no se trata de un listado exhaustivo, sí es un esfuerzo por explicar el alcance de la recolección y, por tanto, sirve para informar a las personas que usan sus servicios. Movistar señala que dichas finalidades apuntan a satisfacer un "beneficio propio o de terceros" con los que la empresa haya suscrito acuerdos de envío o recepción de la información teniendo en cuenta la autorización de la persona usuaria para ello.

En el acceso a los datos de las personas que suscriben sus servicios en el marco de relaciones comerciales, Movistar puede compartir dichos datos con entidades financieras con las que celebra convenios o terceras empresas con fines comerciales o publicitarios, ya sea en Colombia o en el exterior.

Tigo informa en su política de protección de datos que recoge datos de las personas que usan sus servicios incluyendo nombre, teléfono, dirección de correo electrónico, información de pago, dirección de facturación o usuario y la contraseña, información sobre el uso de su portal web, así como "la dirección de red y el sistema operativo de la computadora utilizada, tipo de navegador, el sitio web desde el cual el cliente se vinculó a nuestro portal, la actividad en nuestro portal, así como el historial de visualización, la hora y la fecha en la cual el cliente visitó el portal y compró productos y servicios a través del portal; información sobre la ubicación del cliente; información del uso de aplicaciones móviles según los sitios web visitados y las aplicaciones descargadas en la red TIGO". Entre los operadores evaluados, es el que precisa con mayor granularidad el tipo de datos que recolecta.

Tigo además informa mediante qué canales recolecta esa información y sobre los usos que da a dichos datos. Sobre el envío y acceso a los datos de las personas que usan sus servicios con aliados comerciales, Tigo precisa que podrá hacerlo con entidades afiliadas a dicha compañía, en caso de fusión, adquisición, venta de activos, entre otros eventos. Y siempre que medie una autorización expresa e inequívoca, sin que exista un criterio distinto al de la autorización de la persona para hacerlo.

ETB en su política de tratamiento de datos si bien no advierte qué datos en concreto recoge salvo la distinción genérica de dato público, semiprivado y sensible, señala de manera precisa para qué fines los recolecta según se trate de las personas que usan sus servicios, las que trabajan para la empresa, y sus accionistas.

Entre las finalidades para el tratamiento de datos de las personas que usan sus servicios incluye "toda la gestión contractual (...) gestión de la orden de compra, instalación, configuración, modificación, desconexión, reconexión y retiro de los servicios (...)" así como "compartir la información a terceros en virtud de obligaciones legales o regulatorias".

Es más, Etb advierte finalidades adicionales si se trata de potenciales clientes, incluyendo como fines del tratamiento la "gestión de acciones necesarias para cumplir los fines de mercadeo, tales como comunicar eficientemente información propia de ETB, así como de nuestras filiales y/o aliados comerciales, sobre productos (...) participar en programas de lealtad con beneficios (...), realizar estudios de mercadeo sobre hábitos de consumo, transferir y transmitir datos personales a terceros con vínculos comerciales con ETB (...)" entre otros. No delimita ningún criterio para compartir los datos de las personas suscritas a sus servicios o que potencialmente se suscribirán, con aliados comerciales.

DirecTV hace público tanto su manual interno de políticas y procedimientos sobre tratamiento de datos personales, como su política de tratamiento de datos.

En esta última señala que recoge información sobre: la cuenta de las personas que usan sus servicios, del servicio, de observación anónima, diagnóstica, comercial, del sitio web e información personal a través de cookies.

En el manual interno de políticas y procedimientos para el tratamiento de datos, advierte que, entre los usos o fines para los que emplea la información recolectada de las personas que usan sus servicios, se encuentran las actividades de mercadeo, promoción y publicidad propia o de terceros, venta, facturación, gestión de cobranza, recaudo, programación, soporte técnico, inteligencia de mercados, mejoramiento del servicio, entre otras.

Luego, en su política de tratamiento de datos, el proveedor de servicios de internet y telefonía celular advierte las razones por las que comparte con aliados comerciales los datos de las personas que se suscriben a sus servicios. El listado no taxativo incluye los servicios de apoyo, en los que comparte esos datos para el procesamiento de facturas, asistencia técnica, y otros. En los servicios que recibe de parte de terceros, comparte los datos para poder coordinar el cobro de servicios provistos por éstos. Con sus compañías afiliadas, señala que es necesario que las personas usuarias de sus servicios consientan para compartir sus datos. Para fines de mercadeo dice que podría compartir información con proveedores y terceros en caso de venta u otro tipo de transferencia de los activos de DirecTV.

Avantel en su política de tratamiento de datos desagrega los tipos de datos que recoge de las personas que son usuarias de sus servicios al incluir datos generales referentes a su condición de mayoría de edad, datos de identificación, "inclusive biométricos (imagen y voz)", datos de ubicación privada y comercial, datos socioeconómicos como los datos patrimoniales de la persona. Esa granularidad también la aplica al referirse a los datos de quienes son sus proveedores, personas que trabajan para ella, terceros colaboradores, terceros visitantes así como terceros en procesos de selección.

Sobre las finalidades o usos para los que emplea los datos de las personas que suscriben sus servicios, Avantel señala un listado más o menos extenso que incluye la verificación de antecedentes comerciales, reputacionales y eventuales riesgos de relacionamientos asociados al lavado de activos y financiación del territorismo, el desarrollo de actividades de marketing e inteligencia de mercados, entre otros.

En su vínculo con aliados comerciales Avantel hace público un compromiso que creemos que constituye una buena práctica que debiera poder ser imitada por el resto de actores en el sector.

Advierte que procurará "vincularse y relacionarse laboral o comercialmente con aquellos terceros que reflejen su compromiso con la observancia y aplicación del régimen general de protección de datos personales en su respectiva operación". Como requisitos para el intercambio de datos con aliados comerciales, Avantel prevé que "deberán acreditar de manera previa al momento de su vinculación, el cumplimiento de los requisitos del régimen de protección de datos, incluyendo pero sin limitarse a la existencia y aplicación de una política de tratamiento de datos personales, la habilitación de canales para la atención de consultas y reclamos para los titulares de información personal, así como la efectiva realización y actualización del Registro Nacional de Bases de Datos Personales ante la Superintendencia de Industria y Comercio".

Avantel de manera novedosa con relación al resto de operadores, dice que se reserva el derecho de supervisar de manera periódica el cumplimiento de los requisitos legales y contractuales asociados al régimen de protección de datos personales por parte de terceros con los que sostiene un vínculo comercial. Y que en el marco de esa supervisión, solicitará evidencias o soportes de cumplimiento, "realizar visitas periódicas o sedes del tercero, entre otras medidas que estime razonable acorde con la criticidad de la operación, el volumen de los datos o la naturaleza del objeto contractual.

RECOMENDACIONES

1 Pensamos que los operadores podrían ser más claros sobre qué significa que harán tratamiento de datos para beneficio propio o de terceros. Se puede explicar mejor en qué consisten estos convenios con terceros.

2 Avantel incluye una buena práctica sobre las condiciones que rigen en su relacionamiento con aliados comerciales en materia de protección de datos que creemos puede servir como ejemplo. Los mecanismos de verificación de prácticas de tratamiento de datos entre los operadores y sus aliados, así como condicionar dicho relacionamiento al cumplimiento de las obligaciones que tienen a cargo en esa materia, debe apuntar a la mejor protección de la privacidad de las personas suscriptoras de los servicios que éstas ofrecen.

3 lRecomendamos que la fórmula genérica sobre los datos que recogen algunos operadores, que se reduce a afirmar que son datos públicos, semiprivados y sensibles -entre otros-, debería desglosarse ofreciendo más detalle y granularidad. Es decir, debería desagregarse según el tipo de dato que se recoge y advertir cuál es el fin para el que la empresa los usa.

4 Otros criterios evaluados

Entre otros criterios que evaluamos en nuestro informe, incluimos en el eje de compromisos políticos la evaluación de la política de género y la política de accesibilidad de las empresas. Y dedicamos por último, un eje en seguridad digital en el que evaluamos la información en relación con los procedimientos para prevenir y hacer frente a fugas de datos y las acciones de mitigación que siguen a eventos de esa naturaleza, y validamos por último que los sitios web de los operadores cuenten con el protocolo https en sus sitios web.

Compromisos políticos

En este eje se revisan las políticas internas de cada compañía respecto al trato con sus trabajadores. Revisamos qué factores tienen en cuenta para la selección y contratación de personal, el desarrollo de carreras incluyendo capacitación y ascensos a puestos directivos, los beneficios y equilibrio familiar-laboral, la prevención del acoso sexual en los entorno laborales y la promoción de imágenes públicas no sexistas. Esta información la consultamos bien en políticas separadas de género o en los informes de transparencia de cada compañía.

Movistar, **Claro** y **ETB** puntean como las compañías con las políticas de inclusión de género y oportunidades para sus trabajadores que atienden en mejor medida las buenas prácticas que evaluamos. Les siguen **Tigo** y **DirecTV** que abordan más o menos algunas de estas políticas y criterios.

Claro cuenta con una universidad y centro de capacitaciones para su personal empleado por lo que tiene programas de desarrollo de carreras y ascensos. Cuenta con políticas de equilibrio y bienestar familiar entre las que se encuentran licencias de maternidad y paternidad, eventos de reunión familiar, entre otros. Tiene una política de inclusión y diversidad. Esta empresa recibe este año una bonificación por integrar lenguaje incluyente.

Movistar provee oportunidades de capacitación para su personal, tiene políticas de inclusión y diversidad hasta políticas de contratación basadas en el mérito así como una política de género y código de ética que abordan los procedimientos y prácticas para evitar el acoso sexual. En su política de desarrollo de carreras para colaboradores la empresa recibe bonificación por integrar en ese documento lenguaje incluyente.

ETB etalla en su reporte integrado de gestión que cuenta con una política de selección, contratación y promoción del empleo con enfoque de género, así como con una escuela corporativa para el desarrollo de carreras. Cuenta con programas que promueven el bienestar familiar y con un comité de convivencia laboral encargado de desplegar acciones de prevención del acoso laboral.

Tigo cuenta con políticas de prevención de acoso sexual, así como con un programa de desarrollo profesional y prácticas de selección y contratación de personal que promueven la diversidad sexual y de género. No encontramos políticas sobre equilibrio familiar e igualdad en beneficios.

DirecTV posee una política de diversidad e inclusión donde buscan que sus equipos estén compuestos por personas de origen, orientación y género diverso. En su código de ética relacionan la existencia de mecanismos de prevención del acoso sexual, así como de selección y contratación con enfoques que promuevan la participación de personas sin importar su origen, su inclinación u orientación sexual o identidad de género.

EmCali y **Avantel** no publican aún información relacionada sobre políticas de este tipo.

Política de accesibilidad

En este se evalúa si la página web cuenta con una versión accesible para personas con discapacidad visual y baja visión.

EmCali si bien no cuenta con una política de accesibilidad tiene en su página web una opción que permite configurar el contraste en este espacio y así facilitar el acceso a personas con discapacidad visual.

Movistar por su parte, cuenta con una política de accesibilidad que está publicada en su página web y tiene un botón habilitado en su portal para habilitar el ingreso en condiciones que sean accesibles a las personas con discapacidad, para ello solicita que la persona instale un software lector o magnificador pantalla de manera gratuita y provee las indicaciones sobre cómo hacerlo. El resto de operadores no tienen aún políticas públicas de accesibilidad o configuraciones de accesibilidad como las de EmCali y Movistar.

Seguridad digital

En este eje, se evalúa si las compañías informan las fugas de datos personales y acciones de mitigación en caso de que se presenten, si tienen protocolos de notificación a las autoridades cuando presentan fallas de seguridad, así como de notificación a las personas usuarias si esto sucede y también se analiza si dan información sobre las medidas que asumirán cuando se presente un inconveniente. Esta información la verificamos en las políticas de protección de datos de las empresas. También tomamos nota de los portales web de cada operador y que en efecto usen un protocolo de seguridad https.

Mientras que todos los operadores han incluido el certificado de seguridad en sus portales, solo tres operadores entre los siete evaluados cuentan con políticas públicas para el manejo de fugas de datos. **Movistar**, **Tigo** y **Avantel** son las únicas que cuentan con un protocolo y documentación para realizar acciones de mitigación y bloqueos.

Movistar advierte en su Centro de Privacidad que notifica a las autoridades ante eventos de fuga, que notifica a sus suscriptores y que hará públicas las acciones empleadas para la mitigación.

Tigo expresa en su documento titulado "Requerimiento de datos personales por terceros y bloqueos de contenido" que ante incidentes de seguridad cumplirá con la obligación legal de reportarlo ante la Superintendencia de Industria y Comercio, así como notificará a sus suscriptores de un "mecanismo eficaz (...) y las medidas realizadas por la compañía para disminuir el riesgo".

Avantel prevé en su política de tratamiento de datos que notificará a la autoridad cuando "se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares", así mismo asume como deber "informar y apoyar el responsable en la gestión de incidentes de seguridad de la información que comprometan información personal de los cuales tenga conocimiento o que sean informados al responsable". Si bien no expresa que notificará a sus suscriptores sobre eventos de este tipo, sí señala que emprenderá las acciones de mitigación que sean pertinentes en cada caso.

RECOMENDACIONES

1. Esperamos que en la próxima edición de nuestro informe las empresas puedan contarnos qué ajustes razonables despliegan para hacer posible los derechos de las personas con discapacidad para acceder a sus contenidos, especialmente ahora en vigencia de la Ley 1996 de 2020 que reconoce y amplía las obligaciones a cargo de las personas que en el ámbito público y privado deben permitir el ejercicio pleno y autónomo de sus derechos.

2. Es un deber legal de los operadores notificar a la autoridad de protección de datos cuando se presentan eventos que exponen la seguridad de los datos de las personas suscritas a sus servicios (Ley 1581 de 2012, lit. n). Adicionalmente, desde hace años el gobierno está trabajando en una política que haga que estos informes sean más detallados, con plazos y que incluyan otras autoridades, algo que ya sucede en otros países y que podría ser un compromiso empresarial. Igualmente, aunque no hay una obligación legal aún de informar a las personas afectadas sobre los incidentes o los procedimientos para atenderlos este debería ser un compromiso empresarial que reconozca que las personas tienen derecho de conocer cuándo su información ha sido expuesta por brechas de seguridad, y a saber cuáles son las acciones de mitigación desplegadas por parte del responsable del tratamiento para cuidar y proteger sus datos. Por tanto, esperamos que los operadores que aún no comunican sobre estos procedimientos puedan contar qué hacen y cómo ante eventos de fuga de datos para la próxima edición de este informe. Además, que incrementen o instalen mejores políticas sobre diversidad e inclusión que otorguen mejores herramientas para el bienestar de sus trabajadores.

LAS GRÁFICAS ¿DÓNDE ESTÁN MIS DATOS?

Los datos de la evaluación de cada empresa se reflejan en las siguientes gráficas:



	Claro	ETB (EM)	movistar	tigo	eTb	D	A
1. Compromisos políticos	2	2	4	1	1	0	0
2. Intimidad	2	0	3	2	1	2	2
3. Libertad de expresión	3	0	4	3	3	3	3
4. Seguridad digital	3	2	4	4	2	2	4

	Claro	EM	movistar	tigo	eTb		
1. Compromisos políticos	**2**	**2**	**4**	**1**	**1**	**0**	**0**
1.1. Política de género	*						
1.2. Política de accesibilidad							
1.3. Informes de transparencia							
2. Intimidad	**2**	**0**	**3**	**2**	**1**	**2**	**2**
2.1. Políticas de protección de datos							
2.2. Informa la obligación legal de retención de datos							
2.3. Informa las razones para responder a solicitudes de información del sector público							
2.4. Procedimiento de entrega de datos al sector público							
2.5. Notifica a las personas sobre la entrega de datos a entidades públicas							
2.6 Criterios para el tratamiento de datos en relación con aliados comerciales							
3. Libertad de expresión	**3**	**0**	**4**	**3**	**3**	**3**	**3**
3.1. Informa sobre la obligación legal de bloqueo							
3.2 Procedimientos de bloqueo (incluye obligación contractual)							
3.3. Guía sobre comportamientos no permitidos							
4. Seguridad digital	**3**	**2**	**4**	**4**	**2**	**2**	**4**
4.1. Informa de fuga de datos personales y acciones de mitigación							
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web							

*Claro recibe bonificación parcial en tanto que en la política de género algunos de sus documentos cuentan con lenguaje incluyente..

Claro	Suma por criterio	Promedio por eje 2019	Promedio por eje 2020
1. Compromisos políticos		2	2
1.1. Política de género			
1.2. Política de accesibilidad			
1.3. Informes de transparencia			
2. Intimidad		2	2
2.1. Políticas de protección de datos			
2.2. Informa la obligación legal de retención de datos			
2.3. Informa las razones para responder a solicitudes de información del sector público			
2.4. Procedimiento de entrega de datos al sector público			
2.5. Notifica a las personas sobre la entrega de datos a entidades públicas			
2.6. Criterios para el tratamiento de datos en relación con aliados comerciales			
3. Libertad de expresión		3	3
3.1. Informa sobre la obligación legal de bloqueo			
3.2 Procedimientos de bloqueo (incluye obligación contractual)			
3.3. Guía sobre comportamientos no permitidos			
4. Seguridad digital		2	3
4.1. Informa de fuga de datos personales y acciones de mitigación			
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web			

	Suma por criterio	Promedio por eje	
		2019	**2020**
1. Compromisos políticos		**2**	**1**
1.1. Política de género			
1.2. Política de accesibilidad			
1.3. Informes de transparencia			
2. Intimidad		**0**	**1**
2.1. Políticas de protección de datos			
2.2. Informa la obligación legal de retención de datos			
2.3. Informa las razones para responder a solicitudes de información del sector público			
2.4. Procedimiento de entrega de datos al sector público			
2.5. Notifica a las personas sobre la entrega de datos a entidades públicas			
2.6. Criterios para el tratamiento de datos en relación con aliados comerciales			
3. Libertad de expresión		**3**	**3**
3.1. Informa sobre la obligación legal de bloqueo			
3.2 Procedimientos de bloqueo (incluye obligación contractual)			
3.3. Guía sobre comportamientos no permitidos			
4. Seguridad digital		**2**	**2**
4.1. Informa de fuga de datos personales y acciones de mitigación			
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web			

DIRECTV	Suma por criterio	Promedio por eje 2019	Promedio por eje 2020
1. Compromisos políticos		**1**	**0**
1.1. Política de género			
1.2. Política de accesibilidad			
1.3. Informes de transparencia			
2. Intimidad		**2**	**2**
2.1. Políticas de protección de datos			
2.2. Informa la obligación legal de retención de datos			
2.3. Informa las razones para responder a solicitudes de información del sector público			
2.4. Procedimiento de entrega de datos al sector público			
2.5. Notifica a las personas sobre la entrega de datos a entidades públicas			
2.6. Criterios para el tratamiento de datos en relación con aliados comerciales			
3. Libertad de expresión		**0**	**3**
3.1. Informa sobre la obligación legal de bloqueo			
3.2 Procedimientos de bloqueo (incluye obligación contractual)			
3.3. Guía sobre comportamientos no permitidos			
4. Seguridad digital		**2**	**2**
4.1. Informa de fuga de datos personales y acciones de mitigación			
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web			

tigo

	Suma por criterio	Promedio por eje 2019	Promedio por eje 2020
1. Compromisos políticos		**1**	**1**
1.1. Política de género			
1.2. Política de accesibilidad			
1.3. Informes de transparencia			
2. Intimidad		**3**	**2**
2.1. Políticas de protección de datos			
2.2. Informa la obligación legal de retención de datos			
2.3. Informa las razones para responder a solicitudes de información del sector público			
2.4. Procedimiento de entrega de datos al sector público			
2.5. Notifica a las personas sobre la entrega de datos a entidades públicas			
2.6. Criterios para el tratamiento de datos en relación con aliados comerciales			
3. Libertad de expresión		**4**	**3**
3.1. Informa sobre la obligación legal de bloqueo			
3.2 Procedimientos de bloqueo (incluye obligación contractual)			
3.3. Guía sobre comportamientos no permitidos			
4. Seguridad digital		**2**	**4**
4.1. Informa de fuga de datos personales y acciones de mitigación			
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web			

EMCALI VALORAMOS LO ESENCIAL	Suma por criterio	Promedio por eje 2019	Promedio por eje 2020
1. Compromisos políticos		1	2
1.1. Política de género			
1.2. Política de accesibilidad			
1.3. Informes de transparencia			
2. Intimidad		0	0
2.1. Políticas de protección de datos			
2.2. Informa la obligación legal de retención de datos			
2.3. Informa las razones para responder a solicitudes de información del sector público			
2.4. Procedimiento de entrega de datos al sector público			
2.5. Notifica a las personas sobre la entrega de datos a entidades públicas			
2.6. Criterios para el tratamiento de datos en relación con aliados comerciales			
3. Libertad de expresión		0	0
3.1. Informa sobre la obligación legal de bloqueo			
3.2 Procedimientos de bloqueo (incluye obligación contractual)			
3.3. Guía sobre comportamientos no permitidos			
4. Seguridad digital		2	2
4.1. Informa de fuga de datos personales y acciones de mitigación			
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web			

Avantel LTE PRO	Suma por criterio	Promedio por eje 2019*	Promedio por eje 2020
1. Compromisos políticos			**0**
1.1. Política de género			
1.2. Política de accesibilidad			
1.3. Informes de transparencia			
2. Intimidad			**2**
2.1. Políticas de protección de datos			
2.2. Informa la obligación legal de retención de datos			
2.3. Informa las razones para responder a solicitudes de información del sector público			
2.4. Procedimiento de entrega de datos al sector público			
2.5. Notifica a las personas sobre la entrega de datos a entidades públicas			
2.6. Criterios para el tratamiento de datos en relación con aliados comerciales			
3. Libertad de expresión			**3**
3.1. Informa sobre la obligación legal de bloqueo			
3.2 Procedimientos de bloqueo (incluye obligación contractual)			
3.3. Guía sobre comportamientos no permitidos			
4. Seguridad digital			**4**
4.1. Informa de fuga de datos personales y acciones de mitigación			
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web			

*La compañía se incluyó en este informe desde el año 2020, por tanto, no se reportan datos para el 2019.

movistar	Suma por criterio	Promedio por eje	
		2019	**2020**
1. Compromisos políticos		**4**	**4**
1.1. Política de género			
1.2. Política de accesibilidad			
1.3. Informes de transparencia			
2. Intimidad		**3**	**3**
2.1. Políticas de protección de datos			
2.2. Informa la obligación legal de retención de datos			
2.3. Informa las razones para responder a solicitudes de información del sector público			
2.4. Procedimiento de entrega de datos al sector público			
2.5. Notifica a las personas sobre la entrega de datos a entidades públicas			
2.6. Criterios para el tratamiento de datos en relación con aliados comerciales			
3. Libertad de expresión		**4**	**4**
3.1. Informa sobre la obligación legal de bloqueo			
3.2 Procedimientos de bloqueo (incluye obligación contractual)			
3.3. Guía sobre comportamientos no permitidos			
4. Seguridad digital		**4**	**4**
4.1. Informa de fuga de datos personales y acciones de mitigación			
4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web			

Informe

DÓNDE ESTÁN MIS DATOS



Informe de:

Fundación Karisma

con el apoyo de:



El informe ¿Dónde están mis datos? 2020 es la sexta publicación que realiza la Fundación Karisma de esta serie.

Esta investigación busca que las empresas proveedoras de internet ofrezcan más información a sus usuarios para que mejoren su capacidad de hacer efectivos sus derechos humanos.

Puedes conocer los informes anteriores en https://karisma.org.co/DEMD/

 karisma.org.co

  @fundacionkarismaa

 Fundación Karisma

 @Karisma

 @karismacol